

UNITED STATES DISTRICT COURT

for the
Northern District of Mississippi

In the Matter of the Search of

Toshiba laptop, model # L455D-S5976;
Seagate Barracuda 80 gig hard drive, model
ST380021A, serial # 3HVO8L4N; Mini
laptop, no brand name, model # PC703;
Samsung Tracphone, model # SCH-R375C,
FCC ID # A3LSCHR375C; LG cell phone,
model # VX8360, serial # 901CYCV0276099;
Motorola cell phone, model W755, FCC ID#
IHDT56JB1; Motorola cell phones, model
W755, FCC ID# IHDT56JB1; PNY Flash Drive,
4GB; PNY Flash Drive, 16 GB; SanDisk Flash
Drive, 16GB; LG Flash Drive, 1 GB – Serial
Number 707NMFBT7739; Two SanDisk SDHC
Memory Cards, 16 GB; PNY SDHC Memory
Card, 8GB; Sony CD-R Disc, 700MB; Three
Sony DVD-R Discs, 2.8 GB

Case No. 3:13 MJ 020-SAA

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (*identify the person or describe the property to be searched and give its location*):

See Attachment "A"

located in the Northern District of Mississippi, there is now concealed (*identify the person or describe the property to be seized*):

See Exhibit "B"

The basis for the search under Fed. R. Crim. P. 41(c) is (*check one or more*):

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☐ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

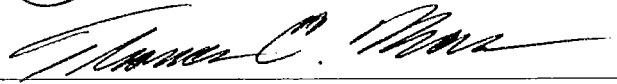
<i>Code Section</i>	<i>Offense Description</i>
18 U.S.C. § 871	Threats against the President and Successors to the Presidency of the United States
18 U.S.C. § 876(C)	Mailing threatening communications

The application is based on these facts:

See Affidavit (Attachment "C")

☒ Continued on the attached sheet.

Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested
under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.



Applicant's signature

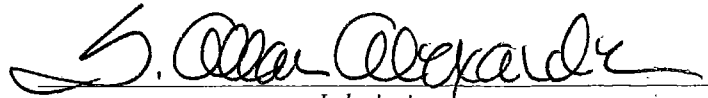
S/A Thomas E. Mann, FBI

Printed name and title

Sworn to before me and signed in my presence.

Date: April 24, 2012

City and state: Oxford, MS



Judge's signature

S. Allan Alexander

United States
Magistrate Judge

ATTACHMENT A

The following "Electronic Devices" to be searched include:

- A. A Toshiba laptop, model # L455D-S5976, serial # Y9O78248K. This laptop contains a Western Digital 160 gig hard drive, serial # WXE408HP5110.
- B. A Seagate Barracuda 80 gig hard drive, model # ST380021A, serial # 3HVO8L4N.
- C. A Mini laptop, no brand name, model # PC703, no serial number, made in China.
- D. A wireless telephone, that is a Samsung Tracphone, model # SCH-R375C, FCC ID # A3LSCHR375C.
- E. A wireless telephone, that is a LG cell phone, model # VX8360, serial # 901CYCV0276099.
- F. A grey colored wireless telephone, that is a Motorola cell phone, model W755, FCC ID# IHDT56JB1
- G. A plum colored wireless telephone, that is a Motorola cell phones, model W755, FCC ID# IHDT56JB1
- H. PNY Flash Drive, 4GB
- I. PNY Flash Drive, 16 GB
- J. SanDisk Flash Drive, 16GB
- K. LG Flash Drive, 1 GB – Serial Number 707NMFBT7739
- L. Two SanDisk SDHC Memory Cards, 16 GB
- M. PNY SDHC Memory Card, 8GB
- N. Sony CD-R Disc, 700MB, "Mix" written in black permanent marker
- O. Three Sony DVD-R Discs, 2.8 GB, no label

The Electronic Devices are currently located at the Tupelo Mississippi Police Department.

ATTACHMENT B

1. All records on the Electronic Devices described in Attachment A that relate to violations of the "TARGET OFFENSES," which includes violations of Title 18, United States Code, Sections 871 and 876(c). For the reasons set out in this affidavit, there is probable cause to believe that the TARGET OFFENSES have been committed by JAMES EVERETT DUTSCHKE. The Electronic Device information includes

- a. Records, documents, programs, applications, or materials relating to biological or chemical weapons, including research for the production of, and records of purchase of ingredients for production of, or otherwise relating to, biological agents, toxins, or delivery systems for the same, including but not limited to ricin, castor beans, and castor plants (*Ricinus Communis*), and pre-cursor items used to produce biological agents.
- b. Records, documents, programs, applications, or materials relating to the handling, use, storage, and disposal of biological or chemical weapons, including biological agents, toxins, or delivery systems for the same, including but not limited to ricin, castor beans, and castor plants (*Ricinus Communis*).
- a. Records, documents, programs, applications, or materials relating to conversations, correspondence, reports, articles or research of public and/or political officials.
- d. With respect to any Electronic Device containing evidence falling within the scope of the foregoing search categories, records, documents, programs, applications or materials, or evidence of the absence of the same, sufficient to show the actual user(s) of the Electronic Device.
- e. As used above in paragraphs (a) through (c), the terms records, documents, programs, applications or materials include records, documents, programs, applications or materials created, modified or stored in any form, including in digital form on any Electronic Device and any forensic copies thereof.

SEARCH PROCEDURE FOR DIGITAL DEVICES

2. In searching Electronic Devices or forensic copies thereof, law enforcement personnel executing this search warrant will employ the following procedure:

- a. Law enforcement personnel or other individuals assisting law enforcement personnel (the "search team") will, in their discretion, either search the Electronic Devices on-

site or seize and transport the device(s) to an appropriate law enforcement laboratory or similar facility to be searched at that location. The search team shall complete the search as soon as is practicable but not to exceed 60 days from the date of execution of the warrant. If additional time is needed, the government may seek an extension of this time period from the Court on or before the date by which the search was to have been completed.

- b. The search team will conduct the search only by using search protocols specifically chosen to identify only the specific items to be seized under this warrant.
- c. The search team may subject all of the data contained in each Electronic Device capable of containing any of the items to be seized to the search protocols to determine whether the device or any data thereon falls within the list of items to be seized. The search team may also search for and attempt to recover “deleted,” “hidden” or encrypted data to determine, pursuant to the protocols, whether the data falls within the list of items to be seized.
- d. The search team may use tools to exclude normal operating system files and standard third-party software that do not need to be searched.
- e. If the search team, while searching an Electronic Device, encounters immediately apparent contraband or other evidence of a crime outside the scope of the items to be seized (evidence of “other crimes”), the team shall not continue to search for evidence of other crimes pending further order of the Court and shall make and retain notes detailing how the contraband or other evidence of a crime was encountered, including how it was immediately apparent contraband or evidence of a crime.
- f. If the search determines that an Electronic Device does not contain any data falling within the list of items to be seized, the government will, as soon as is practicable, return the device and delete or destroy all forensic copies thereof.
- g. If the search determines that an Electronic Device does not contain data falling within the list of items to be seized, the government may make and retain copies of such data, and may access such data at any time.
- h. The government may retain an Electronic Device itself, and/or entire forensic copies of it, until further order of the court or one year after the conclusion of the criminal investigation or case (whichever is latest), if the device is determined to be an instrumentality of an offense under investigation. Otherwise, the government must

return the device and delete or destroy all forensic copies thereof. If the search determines that an Electronic Device contains data falling within the list of items to be seized, the government may also retain the device itself, and/or entire forensic copies of it, without further order of the court.

- i. Notwithstanding the above, after the completion of the search of the Electronic Devices, the government shall not access digital data falling outside the scope of the items to be seized absent further order of court.

As used above, the terms “records” and “information” include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.

ATTACHMENT "C"

**IN THE UNITED STATES DISTRICT COURT FOR THE NORTHERN DISTRICT OF
MISSISSIPPI**

AFFIDAVIT IN SUPPORT OF SEARCH WARRANT

I, Thomas Mann, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of property—"Electronic Devices"—which is currently in law enforcement possession, and the extraction from that property of electronically stored information described in Attachment B.

2. I am employed by the Federal Bureau of Investigation and have been employed for approximately one and a half years. I am a "federal law enforcement officer" within the meaning of Federal Rule of Criminal Procedure 41(a)(2)(C), that is, a government agent engaged in enforcing the criminal laws and duly authorized by the Attorney General to request a search warrant. I am currently assigned to a FBI Counterterrorism squad which includes the Mississippi Joint Terrorism Task Force (JTTF) and, as such, I am charged with enforcing federal law. My primary duty and assignment obligates me to apprehend federal criminals.

3. I have participated in terrorism investigations and, among other things, have conducted or participated in surveillances, the execution of search warrants, and debriefings of suspects and informants. Through my training, education and experience, I have become familiar with methods utilized by individuals to commit terrorism crimes. This includes the use of cellular telephones and Electronic Devices.

4. I submit this affidavit in support of an application for a warrant and order pursuant to Federal Rule of Criminal Procedure 41, for the following "Electronic Devices":

- A. A search warrant for a Toshiba laptop, model # L455D-S5976, serial # Y9O78248K. This laptop contains a Western Digital 160 gig hard drive, serial # WXE408HP5110.
- B. A search warrant for a Seagate Barracuda 80 gig hard drive, model # ST380021A, serial # 3HVO8L4N.

- C. A search warrant for a mini laptop, no brand name, model # PC703, no serial number, made in China.
- D. A search warrant for a wireless telephone, that is a Samsung Tracphone, model # SCH-R375C, FCC ID # A3LSCHR375C.
- E. A search warrant for a wireless telephone, that is a LG cell phone, model # VX8360, serial # 901CYCV0276099.
- F. A search warrant for a grey colored wireless telephone, that is a Motorola cell phone, model W755, FCC ID# IHDT56JB1
- G. A search warrant for a plum colored wireless telephone, that is a Motorola cell phones, model W755, FCC ID# IHDT56JB1
- H. PNY Flash Drive, 4GB
- I. PNY Flash Drive, 16 GB
- J. SanDisk Flash Drive, 16GB
- K. LG Flash Drive, 1 GB – Serial Number 707NMFBT7739
- L. Two SanDisk SDHC Memory Cards, 16 GB
- M. PNY SDHC Memory Card, 8GB
- N. Sony CD-R Disc, 700MB, “Mix” written in black permanent marker
- O. Three Sony DVD-R Discs, 2.8 GB, no label

5. I have personally participated in the investigation set forth below. I am familiar with the facts and circumstances of the investigation through my personal participation; from discussions with other FBI agents and law enforcement officers; from my discussions with witnesses involved in the investigation; and from my review of records and reports relating to the investigation. Since this affidavit is being submitted for the limited purpose of securing the above referenced warrant, I have not included details of every aspect of the investigation.

6. Probable cause exists to believe that execution of the above referenced warrant and order will identify evidence of violations of the "TARGET OFFENSES," which includes violations of Title 18, United States Code, Sections 871 and 876(c). Section 871 states in pertinent part:

Whoever knowingly and willfully deposits for conveyance in the mail or for a delivery from any post office or by any letter carrier, any letter, paper, writing, print, missive or document containing any threat to take the life of, to kidnap, or to inflict bodily harm upon the President of the United States...[shall be guilty of an offense against the United States]; and

Section 876(c) states in pertinent part and as read in conjunction with Title 18, United States Code, Section 876 (a):

Whoever knowingly so deposits or causes to be delivered as aforesaid [by the Postal Service according to the direction thereon], any communication with or without a name or designating mark subscribed thereto, addressed to any other person and containing....any threat to injure the person of the addressee or of another shall be [guilty of an offense against the United States]....

7. For the reasons set out in this affidavit, there is probable cause to believe that the TARGET OFFENSES have been committed by JAMES EVERETT DUTSCHKE and that evidence, fruits, or contraband of these offenses can be found on the Electronic Devices to be searched.

8. The applied-for warrant would authorize the forensic examination of the Electronic Devices for the purpose of identifying electronically stored data particularly described in Attachment B.

PROBABLE CAUSE

9. On April 16, 2013, the Jackson Division of the FBI was advised that the United States Senate Mail Facility in Landover, Maryland, identified an envelope which contained a type-written letter and a suspicious granular substance. The letter was addressed to "Snator (sic) Roger Wicker, 555 Dirksen Senate Bldng, Washington DC 20510" with a printed address label. Senator Wicker is an elected official representing the State of Mississippi whose primary residence is in the Northern District of Mississippi. No return address was identified on the envelope and it was postmarked in Memphis, Tennessee, on April 8, 2013.

10. Contained in the envelope was a letter printed on yellow paper containing the following language:

No one wanted to listen to me before.
There are still 'Missing Pieces'
Maybe I have your attention now
Even if that means someone must die.
This must stop.
To see a wrong and not expose it,
is to become a silent partner to its continuance
I am KC and I approve this message

11. Field tests conducted on the suspicious granular substance presumptively provided positive and inconclusive field tests for Ricin. Of the four (4) field tests conducted by the Hazardous Materials Response Team (HMRT), three (3) were positive for a protein, further tests resolved to be Ricin. One (1) field test was inconclusive. Further analysis conducted of the suspicious powder by a member of the LRN in Maryland advised the substance was "highly reactive" by PCR/TRF for Ricin. LRN is an acronym for Laboratory Response Network which is a partnership between the Centers for Disease Control and Prevention, the FBI and the Association of Public Health Laboratories in an effort to ensure an effective laboratory response to bioterrorism by helping to improve the nation's public health laboratory infrastructure, which had limited ability to respond to bioterrorism. Polymerase Chain Reaction (PCR) and Time-Resolved Fluorescence (TRF) are scientific techniques conducted to determine the presence of biological threat agents in a material.

12. The United States Capitol Police queried Senator Wicker's staff for any constituent with the initials "KC" who previously corresponded with the office. This query revealed a constituent named Paul Kevin Curtis, who previously sent multiple communications to Senator Wicker's office in Washington, DC, containing similar verbiage, "This is KEVIN CURTIS and I approve this message". On September 24, 2010, Curtis posted on his blog that he was currently writing a novel about black market body parts that was titled, "Missing Pieces." On December 7, 2011, Curtis sent an e-mail to United States Representative Alan Nunnelee, First Congressional District of Mississippi, that referred to his book "Missing Pieces". Letters to the President [discussed infra], Senator Wicker and a letter to Lee County Mississippi Justice Court Judge Sadie Holland [discussed infra] also make reference to "Missing Pieces." Additional research revealed on April 12, 2013, Curtis posted a photograph on his Facebook page and under the comments for the picture, he included the quote, "To see a wrong and not expose it, is to become a silent partner to its continuance." On his Facebook page, Curtis refers to himself as "KC". The letters described above and below contain the following quote, "To see a wrong and not expose it is to become a silent partner to its continuance."

13. On April 16, 2013, an envelope was identified addressed to United States President Barack Hussein Obama, specifically "President Barak (sic) Hussein Obama, The White House, 1600 Pennsylvania Ave NW, Washington, DC 20500" with a printed address label, containing the same letter (see below) and suspicious granular substance. The suspicious granular substance presumptively field tested positive for Ricin. No return address was identified on the envelope and the envelope was postmarked in Memphis, Tennessee, on April 8, 2013.

14. Contained in the envelope was a letter printed on yellow paper containing the following language:

No one wanted to listen to me before.
There are still 'Missing Pieces'
Maybe I have your attention now
Even if that means someone must die.
This must stop.
To see a wrong and not expose it,
is to become a silent partner to its continuance
I am KC and I approve this message

15. On April 17, 2013, the Jackson Division of the FBI was advised that Sadie Holland, a Justice Court Judge in Lee County, Mississippi, had received a letter on or about April 10, 2013, delivered by the U. S. Postal Service, meeting the same description. The letter was addressed to Sadie Holland at her office in Tupelo, Mississippi. The letter, like the others, contained a printed address label. No return address was identified on the envelope and it was postmarked in Memphis, Tennessee, on April 8, 2013.

16. Contained in the envelope was a letter printed on yellow paper containing the following language:

No one wanted to listen to me before.
There are still 'Missing Pieces'
Maybe I have your attention now
Even if that means someone must die.
This must stop.
To see a wrong and not expose it,
is to become a silent partner to its continuance
I am KC and I approve this message

17. The envelope which contained the above type-written letter also contained a suspicious granular substance. A presumptive field test conducted by the 47th Civil Support Team of the

Mississippi National Guard identified the granular substance as being positive for Ricin. A visual comparison of the granular substance identified in the President Obama, Senator Wicker, and Judge Holland letters revealed all three (3) to contain a similar substance.

18. The above-referenced letters contained the same verbiage, font, style and paper color (yellow).

19. On Friday April 19, 2013, the FBI crime laboratory confirmed that the substances contained in each of the three letters were in fact a crude form of Ricin. Based upon my training and experience, I know that Ricin is a very toxic substance which, if ingested, inhaled, or absorbed, can be fatal. Properly distributed, it could kill numerous people. Ricin poisoning has no known antidote and is extremely difficult to detect as the cause of death. On Friday, April 19, 2013, federal agents searched Curtis' residence and found no evidence of Ricin production.

20. Based upon information received from inspectors with the United States Postal Service, letters deposited into the United States Mail in most, if not all, of the northern counties in the State of Mississippi, including Lee County, will bear a Memphis, Tennessee, post mark unless the depositor requests otherwise. The United States Postal Inspection Service has determined, based upon the codes printed on the back of the envelopes during the mailing process by the USPS, the above referenced letters were placed into the United States Postal System in Tupelo, Mississippi.

21. Curtis was arrested and charged by criminal complaint on April 17, 2013. On Friday, April 19, 2013, federal agents searched Curtis's residence and found no evidence of Ricin production. As the investigation continued, additional information arose, and, on April 23, 2013, based on new information revealed through the ongoing investigation, the criminal complaint against Curtis was dismissed without prejudice, on the government's motion.

22. After his arrest, Curtis identified JAMES EVERETT DUTSCHKE as being another individual also residing in Tupelo, Mississippi, who could have perpetrated the above described mailings. Several of Curtis's family members also identified DUTSCHKE as a possible perpetrator. Curtis and his family members informed the agents that DUTSCHKE and Curtis have known each other for several years and have had a contentious personal relationship which has manifested itself in e-mail traffic and social media postings.

23. On April 19, 2013, law enforcement agents involved in the investigation interviewed a witness who described statements DUTSCHKE has made in the past. Specifically, the witness recalled that, in 2008, DUTSCHKE told the witness that he could manufacture a "poison." DUTSCHKE stated that he could place the poison in envelopes and send them to elected officials. DUTSCHKE concluded by stating that whoever opened these envelopes containing the

“poison” would die. According to the witness, on or about the same occasion, DUTSCHKE made reference to having “a secret knowledge” for “getting rid of people in office.” The witness also disclosed that he had had an altercation with DUTSCHKE after DUTSCHKE made sexual advances toward the witness’ daughter.

24. On April 22, 2013, an FBI Agent witnessed Waste Management personnel recover the garbage receptacle from the curtilage of DUTSCHKE’s residence located on S. Canal Street, Tupelo, Mississippi 38804. FBI and the Mississippi Office of Homeland Security Agents, recovered the trash receptacle and searched the contents. During the search of the trash receptacle’s contents, several items were identified, to include, but not limited to the following: different types of yellow paper, address labels, and a dust mask. Some of the paper appears very similar in color to the above-described letters; however, they are of different shades of yellow. While the address labels that were found are larger than the labels on the threatening letters, it appears that the labels on the letters were cut from a larger label. Thus, the seized labels could have been cut to size and placed on the letters.

25. Additionally, on April 22, 2013, an FBI Mobile Surveillance Team (MST) observed DUTSCHKE enter his former business, Tupelo Taekwondo Plus, located at 102 Rankin Boulevard Extension, Tupelo, Mississippi. DUTSCHKE informed the property manager he needed to recover a fire extinguisher, a mop, and a bucket he left at the location. DUTSCHKE was observed by surveillance personnel removing items from the location and placing them into a red, 1993 Mercury Villager-Sport Van, Tag No. [REDACTED]. After departing the former business location, DUTSCHKE drove a short distance, approximately 100 yards, and was observed discarding several items through the window of the vehicle into a public garbage receptacle. After DUTSCHKE departed the area, personnel from the Jackson Division of the FBI and the Mississippi Office of Homeland Security recovered the items. Observed inside the garbage receptacle were the following items: the box for a Black and Decker Smart Grind coffee grinder, a latex glove box containing gloves, a blue dust mask, and an empty bucket of floor adhesive. Based on the training and experience of the affiant, a coffee grinder could be utilized to develop Ricin by crushing the castor bean. Furthermore, latex gloves and a dust mask could be utilized as personal protective equipment while the castor beans are being crushed to protect the producer from an accidental exposure. The FBI Mobile Surveillance Team observed DUTSCHKE traveling about in Tupelo, Mississippi, in a green 1998 Dodge Grand Caravan-Extended Sport Van on the evening of April 22, 2013.

26. Land records and eyewitnesses establish that JAMES EVERETT DUTSCHKE resides on S. Canal Street, Tupelo, Mississippi, 38804. Records and eyewitnesses also establish that DUTSCHKE also has two vehicles registered in his name and uses a red, 1993 Mercury Villager-Sport Van, Tag No. [REDACTED] Vin# [REDACTED] 2229, and a green 1998 Dodge Grand Caravan-Extended Sport Van, Tag No. [REDACTED] IN [REDACTED]

27. On April 24, 2013, agents obtained records indicating DUTSCHKE ordered castor bean seeds utilizing e-bay and paid for the seeds via paypal. Specifically, DUTSCHKE paid for castor bean seeds on or about November 17, 2012, and on or about December 1, 2012. The United States Postal Service records confirm that the order paid for on December 1, 2012, was mailed on December 3, 2012, and delivered to DUTSCHKE's S. Canal residence on December 5, 2012.

28. Lee County is within the Northern District of Mississippi. The Lee County Sheriff's Office and the Tupelo Police Department, also within Lee County, conducted a joint State investigation of alleged molestation of a minor charges against JAMES EVERETT DUTSCHKE. On January 18, 2013, DUTSCHKE was arrested by State law enforcement officers for the above referenced charge.

29. On January 22, 2013, DUTSCHKE consented to the search of his home, vehicle and business. Pursuant to said consent, on January 22, 2013, Lee County Sheriff's Deputy Len Schafer seized the above-referenced Electronic Devices from DUTSCHKE's home. Deputy Schafer relinquished custody of the Electronic Devices to Tupelo Police Department Detective Brandon Garrett. The Electronic Devices are currently in the possession of the Tupelo Police Department evidence vault. In my training and experience, I believe that the Electronic Devices have been stored in a manner in which its contents are, to the extent material to this investigation, in substantially the same state as they were when the Electronic Devices first came into the possession of the Tupelo Police Department.

30. While the Federal Bureau of Investigation may already have all necessary authority to examine the Electronic Devices, your affiant seeks this additional warrant out of an abundance of caution to be certain that an examination of the Electronic Devices will comply with the Fourth Amendment and other applicable laws.

TECHNICAL TERMS

31. Based on my training and experience, when discussing the Electronic Devices to be searched, I use the following technical terms to convey the following meanings:

- a. Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the

phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books;" sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system ("GPS") technology for determining the location of the device.

- b. Computers: Computers include the following computer hardware, software, and other devices and information.
 - (1) Computer hardware is described as any and all computer equipment, including any electronic devices which are capable of collecting, analyzing, creating, displaying, converting, storing, concealing, or transmitting electronic, magnetic, optical, or similar computer impulses or data. These devices include, but are not limited to, any data-processing hardware (such as central processing units, memory typewriters, and self-contained "laptop" or "notebook" computers); internal and peripheral storage devices (such as fixed disks, external hard disks, floppy disk drives and diskettes, tape drives and tapes, optical storage devices and other memory storage devices); peripheral input/output devices (such as keyboards, printers, scanners, plotters, video display monitors, and optical readers); and related communications devices (such as modems, cable and connections, recording equipment, RAM or ROM units, acoustic couplers, automatic dialers, speed dialers, programmable telephone dialing or signaling devices, and electronic tone-generating devices); as well as any devices, mechanisms, or parts that can be used to restrict access to such hardware (such as physical keys and locks).
 - (2) Computer software is described as any and all information, including any instructions, programs, or program code, stored in the form of electronic, magnetic, optical, or other media which are capable of being interpreted by a computer or its related components. Computer software may also include certain data, data fragments, or control characters integral to the operation of computer software. This software commonly includes operating systems, other programs/applications (such as word-processing, graphics, spreadsheet, and database programs, and accounting and tax preparation software), utilities, compilers, interpreters, and communications programs.
 - (3) Computer passwords and data security devices are described as all those devices, programs, or data, whether themselves in the nature of hardware or software, that can

be used or is designed for use to restrict access to or facilitate concealment of any computer hardware, computer software, computer-related documentation, electronic data, records, documents or materials within the scope of this application. These items include but are not limited to any data security hardware (such as any encryption devices, chips, circuit boards and dongles), passwords, data security software or information (such as test keys and encryption codes), and similar information that is required to access computer programs or data or to otherwise render programs or data into a useable form.

- (4) Storage medium: A storage medium is any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, memory cards, CD-ROMs, and other magnetic or optical media.
- (5) Portable media player: A portable media player (or “MP3 Player” or iPod) is a handheld digital storage device designed primarily to store and play audio, video, or photographic files. However, a portable media player can also store other digital data. Some portable media players can use removable storage media. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can also store any digital data. Depending on the model, a portable media player may have the ability to store very large amounts of electronic data and may offer additional features such as a calendar, contact list, clock, or games.
- (6) PDA: A personal digital assistant, or PDA, is a handheld electronic device used for storing data (such as names, addresses, appointments or notes) and utilizing computer programs. Some PDAs also function as wireless communication devices and are used to access the Internet and send and receive e-mail. PDAs usually include a memory card or other removable storage media for storing data and a keyboard and/or touch screen for entering data. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can store any digital data. Most PDAs run computer software, giving them many of the same capabilities as personal computers. For example, PDA users can work with word-processing documents, spreadsheets, and presentations. PDAs may also include global positioning system (“GPS”) technology for determining the location of the device.
- (7) Tablet: A tablet is a mobile computer, typically larger than a phone yet smaller than a notebook, that is primarily operated by touching the screen. Tablets function as wireless communication devices and can be used to access the Internet through cellular networks, 802.11 “wi-fi” networks, or otherwise. Tablets typically contain

programs called apps, which, like programs on a personal computer, perform different functions and save data associated with those functions. Apps can, for example, permit accessing the Web, sending and receiving e-mail, and participating in Internet social networks.

- (8) IP Address: An Internet Protocol address (or simply "IP address") is a unique numeric address used by computers on the Internet. An IP address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet computer must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.
- (9) Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

32. Based on my knowledge, training, and experience, I know that Electronic Devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

33. Based on my knowledge, training, and experience, I know that the contents of Electronic Devices have yielded information that is relevant and material to past investigations of the TARGET OFFENSES. For instance, the contents of wireless telephones may reveal numbers that have been in contact with the cell phones, as well as the calling patterns of DUTSCHKE, thus revealing the possible names of accomplices and other individuals who may have assisted in commission of the TARGET OFFENSES, and the geographic breadth of the suspected TARGET OFFENSES. Today, cellular telephones are digital devices capable of containing evidence, such as records, documents, or materials. In the past, your affiant knows that such devices have contained evidence of the commission of such offenses.

34. Based on my knowledge, training, and experience, I know that individuals involved in offenses such as the TARGET OFFENSES often use computers and other electronic devices to research and store information concerning sources for obtaining materials needed to manufacture Ricin as well as the means of manufacturing Ricin. I also know that individuals

committing the TARGET OFFENSES often use computers and other electronic devices to research, identify and locate potential targets and victims for their crimes. Further, individuals engaged in the TARGET OFFENSES often generate and store threatening communications they send or intend to send on electronic devices and in electronic storage and then print or otherwise generate their communications from those devices. In addition, at this time in this investigation, I believe that the three letters mailed in this case were generated on and printed from one or more electronic device(s).

35. There is probable cause to believe that things that were once stored on the Electronic Devices may still be stored there, for at least the following reasons:

- a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person “deletes” a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.
- b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer’s operating system may also keep a record of deleted data in a “swap” or “recovery” file.
- c. Wholly apart from user-generated files, computer storage media—in particular, computers’ internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory “swap” or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.
- d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or “cache.”

36. Forensic evidence. As further described in Attachment B, this application seeks

permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the Electronic Devices were used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the Electronic Devices because:

- a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created.
- b. Forensic evidence on the Electronic Devices can also indicate who has used or controlled the device. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence.
- c. A person with appropriate familiarity with how the Electronic Devices work may, after examining this forensic evidence in its proper context, be able to draw conclusions about how the Electronic Devices were used, the purpose of their use, who used them, and when.
- d. The process of identifying the exact electronically stored information on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.
- e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

37. Nature of examination. Based on the foregoing, and consistent with Rule

41(e)(2)(B), the warrant I am applying for would permit the examination of the Electronic Devices consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

38. Manner of execution. Because this warrant seeks only permission to examine the Electronic Devices already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.


CONCLUSION

39. I submit that this affidavit supports probable cause for a search warrant authorizing the examination of the Device described in Attachment A to seek the items described in Attachment B.

REQUEST FOR SEALING

40. It is respectfully requested that this Court issue an order sealing, until further order of the Court, all papers submitted in support of this application, including the application and search warrant. I believe that sealing this document is necessary because the warrant is relevant to an ongoing criminal investigation, and not all of the possible targets are known at this time. Premature disclosure of the contents of this affidavit and related documents may have a significant and negative impact on the continuing investigation and may severely jeopardize its effectiveness.

Respectfully submitted,


Thomas Mann, Special Agent
Federal Bureau of Investigation

Subscribed and sworn to before me
on April 24, 2013:


UNITED STATES MAGISTRATE JUDGE